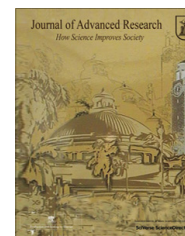




Cairo University Journal of Advanced Research



GUEST EDITORIAL

Special issue on “Cyber Security”



This special issue of the Journal of Advanced Research results from “the US–Egypt Workshop on Cyber Security,” co-sponsored by National Science Foundation (NSF), USA and Scientific Technology Development Authority (STDA), Egypt held in Smart Village, Giza, Egypt on May 27–30, 2013.

After careful reviewing and emphasizing the recent advances in information assurance and network security, this special issue of the Cairo University Journal of Advanced Research, an Elsevier publication, contains three parts with total of nine papers; part I addresses network security, part II focuses on software and applications security, while part III discusses cyber infrastructure protection.

Part I, Network Security, has three papers. The first paper, *DoS Detection in IEEE 802.11 with the Presence of Hidden Nodes*, by Joseph Soryal and Tarek Saadawi presents a novel approach to detect and identify the attacker who is employing denial of service (DoS) attack to disrupt the wireless networks with the presence of hidden nodes employing the widely used IEEE 802.11 DCF protocols. Malicious nodes alter the IEEE 802.11 standards to illicitly capture the channel and increase the probability of successful packet transmission on the expense of innocent nodes that follow the protocol standards. The detection process utilizes the theoretical network throughput derived using two dimensional Markov chain to determine the network capacity and use the results as baseline for detection.

The paper by Jayaram Raghuram, David J. Miller, and George Kesidis titled; *Unsupervised, low latency anomaly detection of algorithmically generated domain names by generative probabilistic modeling*, presents a method for detecting anomalous domain names. The paper focuses on algorithmically generated domain names which are frequently associated with malicious activities such as fast flux service networks, particularly for bot networks (or botnets), malware, and phishing. The method is based on learning a (null hypothesis) probability model based on a large set of domain names that have been white listed by some reliable authority. Since these names are mostly assigned by humans, they are pronounceable, and tend

to have a distribution of characters, words, word lengths, and number of words that are typical of some language (mostly English), and often consist of words drawn from a known lexicon.

The third paper is entitled *An Efficient Method to Detect Periodic Behavior in Botnet Traffic by Analyzing Control Plane Traffic*, by Basil AsSadhan and José M.F. Moura. Botnets pose a significant threat to Internet’s communications and applications. A botnet relies on command and control (C2) communications channels traffic between its members for its attack execution. C2 traffic occurs prior to any attack; hence, the detection botnet’s C2 traffic enables detection of members of the botnet before any real harm happens. The authors analyze C2 traffic and find that it exhibits a periodic behavior. This is due to the pre-programmed behavior of bots that check for updates to download them every T seconds. They exploit this periodic behavior to detect C2 traffic. The statistical testing looks only at aggregate control plane traffic behavior, which makes it more efficient and scalable than techniques that involve deep packet inspection (DPI) or tracking the communication flows of different hosts. They apply the test to two types of botnet; namely tinyP2P and IRC, which are generated by SLINGbot.

Part II, Software and Application Security, has three papers. The paper entitled, *Supporting Secure Programming through Interactive Static Analysis*, by Jun Zhu, Jing Xie, Heather Lipford, and Bill Chu focuses on security incidents that are caused by software developers’ failure to adhere to secure programming practices. Static analysis tools have been used to detect software vulnerabilities. The author approach is interactive static analysis, to integrate static analysis into Integrated Development Environments (IDE) and provide in-situ secure programming support to help developers prevent vulnerabilities during code construction. No additional training is required nor are there any assumptions on ways programs are built. Their work is motivated in part by the observation that many vulnerabilities are introduced due to failure to practice secure programming by knowledgeable developers. The authors implement a prototype interactive static analysis tool as a plug-in for Java in Eclipse. The technical evaluation of the prototype detects multiple zeroday vulnerabilities in a large open source project. The evaluations also suggest that false positives may be limited to a very small class of use cases.

Peer review under responsibility of Cairo University.



Production and hosting by Elsevier

The fifth paper in this special issue is entitled; *Capturing Security Requirements for Software Systems*, by Hassan El-Hadary and Sherif El-Kassas proposes a methodology for security requirement elicitation based on problem frames. The methodology aims at early integration of security with software development. The main goal of the methodology is to assist developers elicit adequate security requirements in a more systematic way during the requirement engineering process. A security catalog, based on problem frames, is constructed in order to help identifying security requirements with the aid of previous security knowledge. Abuse frames are used to model threats while security problem frames are used to model security requirements. The authors have made use of evaluation criteria to evaluate the resulting security requirements concentrating on conflicts identification among requirements. They have shown that more complete security requirements can be elicited by such methodology in addition to the assistance offered to developers to elicit security requirements in a more systematic way.

The paper entitled; *Fast Flux Watch: A Mechanism for Online Detection of Fast Flux Networks*, by Basheer Al-Duwairi and Ahmad Al-Hammouri, proposes Fast Flux Watch (FF-Watch), a mechanism for online detection of fast flux agents. Fast flux networks represent a special type of botnets that are used to provide highly available web services to a backend server, which usually hosts malicious content. Detection of fast flux networks continues to be a challenging issue because of the similar behavior between these networks and other legitimate infrastructures, such as CDNs and server farms. FF-Watch is envisioned to exist as a software agent at leaf routers that connect stub networks to the Internet. The core mechanism of FF-Watch is based on the inherent feature of fast flux networks: flux agents within stub networks take the role of relaying client requests to point-of-sale websites of spam campaigns. Therefore, the main idea of FF-Watch is to correlate incoming TCP connection requests to flux agents within a stub network with outgoing TCP connection requests from the same agents to the point-of-sale website. Theoretical and traffic trace driven analyses show that the proposed mechanism can be utilized to efficiently detect fast flux agents within a stub network.

Part III, Cyber Infrastructure Protection, has three papers. The paper entitled; *Cyber-Physical Security of Wide-Area Monitoring, Protection and Control in a Smart Grid Environment*, by Aditya Ashok α , Adam Hahn and Manimaran Govindarasu addresses cyber security for the smart grid. The paper discusses cyber-physical security of Wide-Area Monitoring, Protection and Control (WAMPAC) from a coordinated cyber attack

perspective and introduces a game-theoretic approach to address the issue. Finally, the paper briefly describes how cyber-physical testbeds can be used to evaluate the security research and perform realistic attack-defense studies for Smart Grid type environments.

The eighth paper in this special issue entitled; *Cyber Security in Smart Cities: Safety, Security and Privacy with the Internet of Things*, by Adel Elmaghraby and Michael Losavio, presents cyber security issues in the smart city. The authors examine two important and entangled challenges: security and privacy. Security includes illegal access to information and attacks causing physical disruptions in service availability. As digital citizens are more and more instrumented with data available about their location and activities, privacy seems to disappear. Privacy protecting systems that gather data and trigger emergency response when needed are technological challenges that go hand-in-hand with the continuous security challenges. Their implementation is essential for a Smart City in which we would wish to live.

Finally, the paper entitled; *System-Level Protection and Hardware Trojan Detection Using Weighted Voting*, by Hany Amin M. Amin, Yousra Alkabani, and Gamal M.I. Selim, discusses the problem of hardware Trojans. Hardware Trojans can be embedded on chip during manufacturing or in third party intellectual property cores (IPs) during the design process. Recent research is performed to detect Trojans embedded at manufacturing time by comparing the suspected chip to a golden chip that is trusted. However, the detection of Trojans in third party IPs is more challenging especially as there is no golden chip to use as reference. This paper proposes a new methodology to detect/prevent Hardware Trojans in third party IPs. The method works by gradually building trust in suspected IPs by comparing outputs of different untrusted implementations of the same IP. Simulation results show that our method achieves higher probability of Trojan detection over a naive implementation of simple voting on the output of different IPs. In addition, experimental results show that our method requires less area and power hardware overhead when compared to a simple voting technique achieving the same degree of security.

Guest Editors

Tarek Saadawi

City University of New York, USA

Ayman El-Desouki

Electronic Research Institute, Egypt